**Keys**

|  |  |  |
| --- | --- | --- |
| **1.** | Which of the following does not use symmetric keys?   1. SEAL 2. DES 3. RC6 4. RSA | [*     D. RSA uses asymmetric keys.  *     A , B , and C use symmetric keys.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=836490962&rowid=1675#answer.N27) |
| **2.** | What kind of RSA key typically decrypts data in a file transfer?   1. Symmetric 2. Public 3. Private 4. Secret | [*     C. Private keys decrypt data.  *    RSA uses asymmetric keys, not symmetric, making A incorrect. B encrypts data. D is a nonexistent symmetric/asymmetric keying term.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=836490962&rowid=1675#answer.N83) |
| **3.** | Which of the following is not true of asymmetric keying algorithms?   1. The private key can be shared without compromising security. 2. They are more complex than symmetric algorithms. 3. They are more secure than symmetric algorithms. 4. They support longer key lengths than symmetric algorithms. | [*     A. The public, not private, key can be shared without compromising security.  *     B , C , and D are true of asymmetric keys and their algorithms.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=836490962&rowid=1675#answer.N140) |
| **4.** | Which of the following is not an example of an asymmetric keying algorithm?   1. DSS 2. Skipjack 3. DH 4. ECC | [*     B. Skipjack uses a symmetric algorithm.  *     A , C , and D are examples of asymmetric algorithms.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=836490962&rowid=1675#answer.N197) |

**Answers**

|  |  |
| --- | --- |
| **1.** | *  **D.** RSA uses asymmetric keys. *  **A**, **B**, and **C** use symmetric keys. |
| **2.** | *  **C.** Private keys decrypt data. *  RSA uses asymmetric keys, not symmetric, making **A** incorrect. **B** encrypts data. **D** is a nonexistent symmetric/asymmetric keying term. |
| **3.** | *  **A.** The public, not private, key can be shared without compromising security. *  **B**, **C**, and **D** are true of asymmetric keys and their algorithms. |
| **4.** | *  **B.** Skipjack uses a symmetric algorithm. *  **A**, **C**, and **D** are examples of asymmetric algorithms. |

**Ciphers**

|  |  |  |
| --- | --- | --- |
| **5.** | Which of the following is not true of 3DES?   1. It encrypts blocks of 64-bit data. 2. It uses ECB and CBC modes. 3. It runs DES three times. 4. It uses a substitution cipher. | [*     D. 3DES uses a block, not a substitution, cipher.  *     A , B , and C are true of 3DES.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=836490962&rowid=1675#answer.N263) |
| **6.** | Which of the following ciphers operates on small chunks of data, typically in bit sizes?   1. Block 2. Stream 3. Transposition 4. Polyalphabetic | [*     B. A stream cipher operates on small chunks of data, typically in bit sizes.  *     A operates on blocks of data. C encrypts data by taking a unit of plaintext characters, commonly called a group, and shifts them in a regular pattern that results in a permutation. D performs substitution using multiple substitution alphabets.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=836490962&rowid=1675#answer.N323) |

**Answers**

|  |  |
| --- | --- |
| **5.** | *  **D.** 3DES uses a block, not a substitution, cipher. *  **A**, **B**, and **C** are true of 3DES. |
| **6.** | *  **B.** A stream cipher operates on small chunks of data, typically in bit sizes. *  **A** operates on blocks of data. **C** encrypts data by taking a unit of plaintext characters, commonly called a group, and shifts them in a regular pattern that results in a permutation. **D** performs substitution using multiple substitution alphabets. |

**Technology Implementation**

|  |  |  |
| --- | --- | --- |
| **7.** | A(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is where small changes in the input data create large changes in the resulting output data.   1. Asymmetric key 2. Avalanche effect 3. Electronic code book 4. Cipher-block chaining | [*     B. An avalanche effect is where small changes in the input data create large changes in the resulting output data.  *     A is used to encrypt and decrypt data or create and verify digital signatures. C divides data into fixed-length blocks, where each block is encrypted separately. D takes each block of data and XORs it with the previous ciphertext block before encrypting it.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=836490962&rowid=1675#answer.N389) |
| **8.** | What takes variable-length input, along with a key, and creates a fixed-length output?   1. Encryption algorithm 2. HMAC function 3. IDEA 4. RC4 | [*     B. An HMAC function takes variable-length input, along with a key, and creates a fixed-length output.  *     A , C , and D take input and produce the same length output.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=836490962&rowid=1675#answer.N445) |
| **9.** | How long are MD5 signatures?   1. 64 bits 2. 112 bits 3. 128 bits 4. 160 bits | [*     C. MD5 signatures are 128 bits in length.  *    Since MD5 signatures are 128 bits in length, answers A , B , and D are incorrect.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=836490962&rowid=1675#answer.N502) |
| **10.** | Which of the following is an example of an HMAC function?   1. Skipjack 2. RC2 3. DH 4. SHA-1 | [*     D. SHA-1 and MD5 are examples of HMAC functions.  *     A , B , and C are examples of encryption algorithms.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=836490962&rowid=1675#answer.N559) |

**Answers**

|  |  |
| --- | --- |
| **7.** | *  **B.** An avalanche effect is where small changes in the input data create large changes in the resulting output data. *  **A** is used to encrypt and decrypt data or create and verify digital signatures. **C** divides data into fixed-length blocks, where each block is encrypted separately. **D** takes each block of data and XORs it with the previous ciphertext block before encrypting it. |
| **8.** | *  **B.** An HMAC function takes variable-length input, along with a key, and creates a fixed-length output. *  **A**, **C**, and **D** take input and produce the same length output. |
| **9.** | *  **C.** MD5 signatures are 128 bits in length. *  Since MD5 signatures are 128 bits in length, answers **A**, **B**, and **D** are incorrect. |
| **10.** | *  **D.** SHA-1 and MD5 are examples of HMAC functions. *  **A**, **B**, and **C** are examples of encryption algorithms. |